Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently amended) A mobile application security system, comprising:

a central computer, in communication with a first host computer and a second host computer, the first and second host computers executing a mobile application that jumps between the first and second host computers during execution and passes through the central computer, ~~for controlling the security of a mobile application;~~

~~one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;~~

the central computer further comprising means for monitoring ~~the~~ security of the mobile application as ~~it~~ the mobile application jumps between the first and second host computers ~~wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer;~~

~~wherein the security monitoring means~~ the means for monitoring further comprisinges, means for inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, ~~means detecting code of the mobile application marked as immutable~~ and means for replacing ~~the~~ immutable code with code known by the central computer to be safe ~~by the central computer~~.

2. (Currently amended) A mobile application security system, comprising:

a central computer, in communication with a first host computer and a second host computer, the first and second host computers executing a mobile application that jumps between the first and second host computers during execution, passing through the central computer, ~~for controlling the security of a mobile application;~~

~~one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;~~

the central computer further comprising means for monitoring ~~the~~ security of the mobile application as ~~it~~ the mobile application jumps between the first and second host computers ~~wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer; and~~

~~wherein the security monitoring means~~ the means for monitoring further comprisinges, means for inspecting an access control list of the mobile application to determine if state data of the mobile application is marked as immutable, ~~means for detecting state data marked as immutable~~ and means for replacing ~~the~~ immutable state data of the mobile application with state data known by the central computer to be safe ~~by the central computer~~.

3. (Currently amended) A mobile application security system, comprising:

a central computer, in communication with a first host computer and a second host computer, the first and second host computers executing a mobile application that jumps between the first and second host computers during execution, passing through the central computer, ~~for controlling the security of a mobile application;~~

~~one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;~~

the central computer further comprising means for monitoring ~~the~~ security of the mobile application as ~~it~~ the mobile application jumps between the first and second host computers ~~wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer;~~

~~wherein the security monitoring means~~ the means for monitoring further comprisinges, means for inspecting an access control list of the mobile application to determine if itinerary data of the mobile application is marked as immutable, and means for replacing ~~the~~ immutable itinerary data with ~~an~~ itinerary data known by the central computer to be safe ~~by the central computer~~.

4. (Currently amended) The system of ~~Claim~~ claim 3, wherein the itinerary data comprises past historical itinerary data.

5. (Currently amended) A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring ~~the~~ security of the mobile application as it jumps between the first and second hosts, including inspecting an access control list of the mobile application to determine if code of the mobile application is marked as immutable, ~~the host computers, wherein the security monitoring further comprises detecting code of the mobile application that is marked as immutable~~ and replacing ~~the~~ immutable code with code known by the central computer to be safe ~~by the central computer~~.

6. (Currently amended) A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring ~~the~~ security of the mobile application as it jumps between the first and second hosts, including inspecting an access control list of the mobile application to determine if state data of the mobile application is marked as immutable, ~~the host computers,~~

~~wherein the security monitoring further comprises detecting a state of the mobile application that is marked as immutable~~ and replacing ~~the~~ immutable state data with state data that is known by the central computer to be safe ~~by the central computer~~.

7. (Currently amended) A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring ~~the~~ security of the mobile application as it jumps between the first and second hosts, including inspecting an access control list of the mobile application to determine if itinerary data of the mobile application is marked as immutable, ~~the host computers, wherein the security monitoring further comprises detecting an itinerary of the mobile application that is marked as immutable~~ and replacing ~~the~~ immutable itinerary data with itinerary data known by the central computer to be safe ~~by the central computer~~.

8. (Currently amended) The method of ~~Claim~~ claim 7, wherein the itinerary data comprises past historical itinerary data.

9-14. (Canceled)

15. (Currently amended) A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring ~~the~~ security of the mobile application as it jumps between the first and second hosts, including ~~the host computers, wherein the security monitoring further comprises:~~

saving ~~the mobile application~~ code of the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and ~~the~~ a host dispatching the mobile application is trusted,

stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted,

replacing the code of the mobile application when the code is marked as immutable and the mobile application has been dispatched in the past, and

saving the code of the mobile application when the code is not marked as immutable.

16. (Currently amended) A mobile application security system, comprising:

a central computer, in communication with a first host computer and a second host computer, the first and second host computers executing a mobile application that jumps between the first and second host computers during execution and passes through the central computer, ~~for controlling the security of a mobile application~~;

~~one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;~~

the central computer further comprising means for monitoring ~~the~~ security of the mobile application as ~~it~~ the mobile application jumps between the first and second host computers

~~wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer;~~

~~wherein~~ the security monitoring means further comprisinges:

means for saving ~~the mobile application~~ code of the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and ~~the~~ a host dispatching the mobile application is trusted,

means for stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted,

means for replacing the code of the mobile application when the code is marked as immutable and the mobile application has not been dispatched in the past, and

means for saving the code of the mobile application when the code is not marked as immutable.

17. (New) A system, comprising:

a server, in communication with a first host computer and a second host computer, the first and second host computers executing a mobile application that jumps between the first and second host computers during execution, passing through the server, the server inspecting an access control list of the mobile application to determine if data of the mobile application is marked as immutable and replacing immutable data with data known by the central computer to be safe to monitor security of the mobile application as the mobile application jumps between the first and second host computers.

18. (New) The system of claim 17, wherein the data of the mobile application is one from the group containing code, state data and itinerary data.

19. (New) The system of claim 17, wherein the server saves immutable data when the mobile application has not been dispatched in the past and a host dispatching the mobile application is trusted.

20. (New) The system of claim 17, wherein the server strips immutable data when the mobile application has not been dispatched in the past and a host dispatching the mobile application is not trusted.

21. (New) The system of claim 17, wherein the server saves data not marked as immutable when a host dispatching the mobile application is trusted.

22. (New) The system of claim 17, wherein the server replaces immutable data when the mobile application has been dispatched in the past.

23. (New) The system of claim 17, wherein the server forwards the mobile application to a receiving host.

24. (New) A method at a server, comprising:

monitoring security of a mobile application as the mobile application jumps between a first host and a second host including:

inspecting an access control list of the mobile application to determine if data of the mobile application is marked as immutable; and

replacing immutable data with data known to be safe.

25. (New) The method of claim 24, wherein the data of the mobile application is one from the group containing code, state data and itinerary data.

26. (New) The method of claim 24, further comprising:

saving immutable data when the mobile application has not been dispatched in the past and a host dispatching the mobile application is trusted.

27. (New) The method of claim 24, wherein replacing comprises replacing immutable data when the mobile application has not been dispatched in the past and a host dispatching the mobile application is not trusted.

28. (New) The method of claim 24, further comprising:

saving data not marked as immutable when a host dispatching the mobile application is trusted.

29. (New) The method of claim 24, wherein replacing comprises replacing immutable data when the mobile application has been dispatched in the past.

30. (New) The method of claim 24, further comprising:

forwarding the mobile application to a receiving host.